METHOD FOR CRYPTOPROTECTION OF TELECOMMUNICATION KNOW-HOW SYSTEMS

Publication number: RU2077113 (C1)
Publication date: 1997-04-10
Inventor(s): BABOSHIN VLADIMIR ALEKSANDROVI [KZ]; MOLDOVYAN ALEKSANDR ANDREEVICH [KZ]; KHUZIN VELDAN ZINUROVICH [KZ]
Applicant(s): VOENNAYA AKADEMIYA SVYAZI [KZ]
Classification:
- international: ***H04L9/00;*** **H04L9/00**; (IPC1-7): H04L9/00
- European:
Application number: RU19950106218 19950419
Priority number(s): RU19950106218 19950419

Abstract not available for **RU 2077113 (C1)**

(19) RU (11) 2 077 113 (13) C1

(51) МПК[6] H 04 L 9/00

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 95106218/09, 19.04.1995

(46) Дата публикации: 10.04.1997

(71) Заявитель:
Военная академия связи

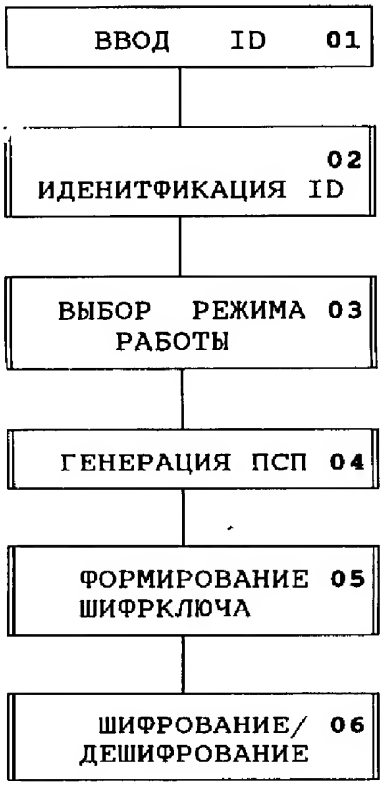
(72) Изобретатель: Бабошин В.А., Молдовян А.А., Хузин В.З.

(73) Патентообладатель:
Военная академия связи

(54) СПОСОБ КРИПТОЗАЩИТЫ СИСТЕМЫ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

(57) Реферат:

Способ относится к электросвязи, а именно к технике криптозащиты систем телекоммуникационных технологий и, в частности, может быть использован в системах и устройствах передачи различных видов информации по каналам электросвязи. Способ криптозащиты системы телекоммуникационных технологий предусматривает предварительную запись совокупности разрешенных паролей, введение пароля, его идентификацию, ввода ключа, генерирование псевдослучайной последовательности, формирование шифроключа, шифрование информационного сигнала, передачу в канал системы связи общего пользования шифрованного сигнала и дешифрования этого сигнала, Устройство криптозащиты систем телекоммуникационных технологий, включает вычислитель 1, блок 2 ввода-вывода, блок 3 алгоритмов, блок 4 хранения ключевых данных, блок 5 сопряжения, блок 6 криптомодуля, шифратор 7, блок 8 управления. Технический результат - высокий уровень защиты данных при их хранении и передаче от дешифрования и возможной модификации за счет криптостойких преобразований, возможность передачи информации как непосредственно с ЭВМ пользователя, так и/или от другого источника информации. 8 з.п.ф., 4 ил.



Фиг. 1

RU 2077113 C1

RU 2077113 C1

(19) **RU** (11) **2 077 113** (13) **C1**

(51) Int. Cl.[6] **H 04 L 9/00**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 95106218/09, 19.04.1995

(46) Date of publication: 10.04.1997

(71) Applicant:
Voennaja akademija svjazi

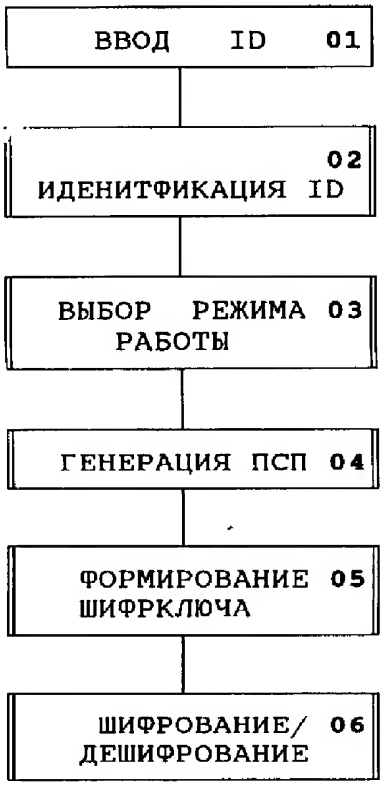
(72) Inventor: Baboshin V.A.,
Moldovjan A.A., Khuzin V.Z.

(73) Proprietor:
Voennaja akademija svjazi

(54) METHOD FOR CRYPTOPROTECTION OF TELECOMMUNICATION KNOW-HOW SYSTEMS

(57) Abstract:

FIELD: electrical communications; devices and systems for transmitting various types of information over electric communication channels. SUBSTANCE: method involves pre-recording of combination of permitted passwords, introduction of password, its identification, introduction of key, generation of pseudorandom train, shaping of crypto key, ciphering of data signal, transmission of crypto signal to shared communication channel and its deciphering. Cryptoprotection system has computer 1, input/output unit 2, algorithm unit 3, key data storage unit 4, interface unit 5, crypto module unit 6, cryptographer 7, control unit 8. EFFECT: improved protection of stored and transmitted data against deciphering and probable modification due to cryptoresistant conversions; provision for data transmission both directly from User's computer and/or from other data source. 9 cl, 4 dwg



Фиг. 1

RU 2077113 C1

RU 2077113 C1

Изобретение относится к электросвязи, а именно к технике криптозащиты систем телекоммуникационных технологий и, в частности, может быть использовано в системах и устройствах передачи различных видов информации по каналам электросвязи.

Известен способ работы аппаратуры передачи данных с защитой от несанкционированного доступа (НДС), заключающийся в том, что на перфокарту установленным способом заносится признак идентификации конкретного пользователя, который считывается специальным устройством и определяется право доступа этого пользователя [1]

Недостатком этого способа является то, что он предназначен, в первую очередь, для защиты от НСД. Кроме того, он не обеспечивает выполнения современных требований к обеспечению гарантированной защиты от НСД, так как предполагает наличие перфокарт, которые могут быть утрачены.

Известен способ передачи секретной информации по системе связи общего пользования, который может быть использован для криптозащиты систем телекоммуникационных технологий. Сущность способа заключается в том, что на приемной станции выбирают простые случайные числа, из которых формируют секретный ключ для приемника в системе связи общего пользования. Из случайных чисел на основе полиноминальных преобразований формируют секретный ключ для дешифрования в приемнике, который непосредственно связан с ключом в системе связи общего пользования для приемника, но не может быть по нему вычислен. Ключ приемника передается на передатчик, который преобразует передаваемую информацию и ключ приемника и формирует зашифрованный сигнал информации. Зашифрованный сигнал передают на корреспондирующий приемник по каналам систем связи общего пользования. Эту информацию легко принять, но невозможно преобразовать без знания секретного ключа дешифрования в приемнике. В приемнике преобразуют зашифрованный сигнал информации и секретный ключ дешифрования в открытое сообщение [2]

Однако существенным недостатком этого способа является низкая производительность, обусловленная необходимостью выполнения полиномиальных преобразований. Кроме того, данный способ не предусматривает защиту информации в процессе ее обработки и хранения.

Наиболее близким к заявленному является способ генерации шифрключа, который может быть использован для криптозащиты систем телекоммуникационных технологий [3]

Известный способ реализован следующим образом: вводят пароль (ID), генерируют шесть значений чисел на основе пароля, например

P_i p_i(ID) mod A

Q_i q_i (ID) mod B

где i=j=1,2,3, а A и B простые числа, формируют матрицу численных значений функций Y и Z размером (A•B). Численные значения функций Y и Z размещают в этой матрице в соответствии с алгоритмами полиномиальных преобразований, в которых числа P_i и Q_i используются в качестве коэффициентов

$Y\ (P_1 + P_2X^2 + P_3X^3)$ mod A,

$Z\ (Q_1Y + Q_2Y^2 + Q_3Y^3)$ mod B

Другие полиномиальные выражения могут быть получены на основе предложенного способа при значениях X 0,1, N-1, где N число битов ключа.

Биты ключа записывают в определенную область запоминающего устройства, идентифицируемую на основе предложенного способа.

Простое число A выбирается как наименьшее простое число, большее на единицу числа N. Если ключ скрыт в области памяти размером M * N бит, простое число B выбирается таким образом, чтобы оно было больше простого числа A и область A*B бит помещалась в области M*N бит.

Формирование множества Y обеспечивается путем расчета функции Y(x) при значениях x 1.(-1), а значения множества Z(Y) рассчитываются по соответствующей формуле, и эти значения размещаются в области памяти по адресам в соответствии с заявляемым способом.

Значения так связаны со значениями позиций бит ключа, 0 и 1 которого записаны в адресуемой области запоминающего устройства, что позволяют провести идентификацию N битного ключа при дешифрации.

Данные, полученные при анализе описания работы способа-прототипа при размещении битов ключа в области памяти, например, размером 2 Кбайта (16000 бит) и при N 64 показывают, что количество вариантов перебора различных значений составит $C_{16000}^{64} = 16000 / 15936$ или примерно 10^{260} комбинаций, что позволяет утверждать о достаточной криптографической стойкости.

Однако известный способ имеет недостатки: обладает невысокой скоростью преобразований, что связано с полиноминальными алгоритмами образования ключа, что вызывает необходимость в проведении сложных вычислений при генерации шифрключа; сформированный ключ используется при обмене информаций по каналам общего пользования, то есть не решается задача защиты информации в процессе ее хранения и обработки.

Целью изобретения является разработка способа криптозащиты телекоммуникационных технологий, обеспечивающего повышение быстродействия, надежности доставки сообщений с гарантированной их защитой при использовании минимального числа дополнительных устройств, обеспечение хранения информации на физическом носителе с гарантированной защитой от несанкционированного доступа.

Это достигается тем, что в известном способе криптозащиты телекоммуникационных технологий, заключающемся в предварительной записи в запоминающее устройство совокупности разрешенных паролей, введения пароля, его идентификации, ввода ключа, генерирования псевдослучайной последовательности,

RU 2077113 C1

RU 2077113 C1

формирования шифрключа, шифрования информационного сигнала, передачи в канал систем связи общего пользования шифрованного сигнала и дешифрования этого сигнала, после идентификации пароля вырабатывают сигнал выбора режима обработки шифрключа и информационного сигнала в системе открытого или закрытого распределения ключей, генерируют псевдослучайную последовательность с использованием выбранной системы распределения ключей, формируют шифрключ в виде подключей заданного размера из псевдослучайной последовательности по выбранному режиму, шифруют информационный сигнал по выбранному режиму, вводят метки сигналов Единого времени, передают зашифрованный информационный сигнал в канал системы связи общего пользования и дешифруют. Причем генерацию псевдослучайной последовательности в системе закрытого распределения ключей осуществляют путем генерации последовательности чисел и наложения на нее пароля, а в системе открытого распределения ключей генерация псевдослучайной последовательности заключается во введении ключей первого X_A и второго X_B корреспондентов, формировании последовательностей по формулам

$Y_A\ q^{XA} \bmod N$,

$Y_B\ q^{XB} \bmod N$,

где q и N параметры открытого ключа, обмене между корреспондентами сформированными последовательностями и вычислении общей последовательности вида

$Y^*\ q^{XAXB} \bmod N$.

Формирование шифрключа из псевдослучайной последовательности в виде подключей заданного размера включает последовательное вычисление значений указателей номера подлежащего обработке блока из псевдослучайной последовательности Y_i и U_i (i 1,2,) по формулам

$Y_i\ [Y_{i-1} + f(U_{i-1})] \bmod (L_y/k)$,

$U_i\ [U_{i-1} + f(U_{i-1})] \bmod (L_u)$

где L и L длины подключей в байтах,определяемых выбранным режимом обработки.

Ввод сигналов Единого времени включает их прием по каналам системы Единого времени, выбор из них временных меток по заданному режиму и записи этих меток в адресные области блоков шифрсигналов.

Шифрование информационного сигнала по заданному режиму включает дискретизацию информационного сигнала на к-байтовые блоки ($K \geq 2$) и преобразование блоков к виду, например $(C_1.C_к)_i\ [(t_1.t_к)_i \mathrm{XORF}\ (Y_i) + f(U_i)] \mathrm{XOR}(p+1)$,

где $(C_1.C_к)$, $(t_1.t_к)$ зашифрованные и исходные информационные сигналы,

p константа, задаваемая выбранным режимом.

Шифрование информационного сигнала по заданному режиму включает дискретизацию информационного сигнала на к-байтовые блоки ($K \geq 2$) и преобразование блоков к виду,например

$(C_1.C_k)\ [t_1.t_k)_i + F(Y_i)] \mathrm{XOR}\ [256f(U_{i-1} + 1)]$

где $(C_1.C_k)$, $(t_1.t_k)$ зашифрованные и исходные информационные сигналы.

Дешифрование зашифрованного сигнала включает дискретизацию принимаемого зашифрованного информационного сигнала на к-битовые блоки ($K \geq 2$), преобразование блоков к виду, например

$(t_1.t_k)_i\ [(C_1.C_k)_i \mathrm{XORF}\ (Y_i) + f(U_i)] \mathrm{XOR}\ (p+1)$,

где $(C_1.C_k)$, $(t_1.t_k)$ зашифрованные и дешифрованные информационные сигналы,

p константа, задаваемая выбранным режимом.

Дешифрование зашифрованного сигнала включает дискретизацию принимаемого зашифрованного информационного сигнала на к-битовые блоки ($K \geq 2$), преобразование блоков к виду, например:

$(t_1.t_k)_i\ (C_1.C_k)_i \mathrm{XOR}[256f(U_{i-1})+f(U_{i-1}+1)]\ F(Y_i)$,

где $(C_1.C_k)$, $(t_1.t_k)$ зашифрованные и дешифрованные информационные сигналы.

На фиг. 1 представлен способ криптозащиты систем телекоммуникационных технологий; на фиг. 2a, 2b способы возможного разбиения ПСП на подключи, формирования из них уникального ключа пользователя и шифрования информации двухбайтовыми блоками; на фиг. 3 способ шифрования четырехбайтовыми блоками; на фиг. 4 устройство, реализующее способ криптозащиты систем телекоммутационных технологий.

Возможность реализации заявляемого способа криптозащиты систем телекоммуникационных технологий объясняется следующим образом.

Первый этап настройки криптомодуля представлен последовательностью процедур на фиг.1 блоками 0,1, 02, 03, 04. С помощью блоков О,1, 02 выполняются процедуры ввода и идентификации пароля. Блок идентификации позволяет определить право доступа пользователя к ресурсам устройства и управлять его полномочиями от полного доступа до абсолютной недоступности в случае несанкционированного доступа. Блок 03 позволяет выбрать режим работы, который заключается в выборе способа генерации псевдослучайной последовательности (ПСП), выборе длины ключа и способа его обработки для получения шифрключа. Блок 04 позволяет сгенерировать ПСП, выбрать ключ заданной длины, записать его для дальнейшего использования.

Генерация псевдослучайной последовательности в предлагаемом способе осуществляется в двух вариантах: в системе закрытого распределения ключей и в системе открытого распределения ключей.

Генерацию псевдослучайной последовательности в системе закрытого распределения ключей осуществляют путем генерации последовательности чисел и наложения на нее пароля.

Генерация псевдослучайной последовательности в системе открытого распределения ключей заключается во введении ключей первого X_A и второго X_B корреспондентов, формировании последовательностей по формулам:

$$Y_A = q^{X_A} \bmod N,$$

$$Y_B = q^{X_B} \bmod N,$$

RU 2077113 C1

RU 2077113 C1

где q и N параметры открытого ключа, обмене между корреспондентами, сформированными последовательностями и вычислении общей последовательности вида

$$Y^{*} = q^{X_A X_B} \bmod N$$

Результатом первого этапа является формирование и запись уникального ключа данного пользователя, который хранится до выключения устройства.

На первом этапе настройки криптомодуля предусмотрены такие процедуры, которые максимально рассеивали бы влияние битов пароля на ключ. Одним из вариантов получения качественной ключевой последовательности на первом этапе является такая схема:

1) простое расширение пароля до необходимой длины для получения исходных данных (предлагается использовать, например, три варианта расширения до 128, 256 или 512 байт);

2) рассеивание влияния символов пароля на конечную ключевую последовательность с помощью шифрования одних исходных ключей под управлением других;

3) наложение порожденного в п.1) шифра на некоторую стандартную случайную последовательность, в результате формируется рабочий ключ, записываемый далее в оперативную память резидентно для управления криптографическими преобразованиями второго этапа.

Рассмотрим варианты алгоритмов, реализующих формирование ключей.

1. Вариант алгоритма генерации ключа, длиной 128 байт.

1.1. Установить значение j 0

1.2. Установить значение i 0

1.3. Записать значение X_n 16 i + j

1.4. Установить i i+1. Если i≧7, то перейти к п.2.3.

1.5. Установить значение j j+1. Если j ≧ 15, то перейти к п.1.2.

1.6. Рассчитать $B = \sum_{k=1}^{1} b_k$, где b_k битовое представление к-того символа пароля.

1.7. Записать a (x + n B) mod 256.

1.8. На полученную последовательность наложить гамму, представляющую собой пароль.

(1.6, 1.7 и 1.8 неустранимые этапы алгоритма, которые многократно повторяются при попытке взломать систему путем подбора пароля; п.п. 1.1,1.5 можно заменить вводом в оперативную память последовательности 0,16, 32, 48, 64, 80, 96, 112, 1,17,113, 2,18,114, 3,19,115; 15,127, а далее перейти к п. п. 6-8).

2. Вариант алгоритма формирования ключа длиной 256 байт.

2.1. Записать последовательность пары чисел i и 255-i для i 0,1,127.

2.2. Полученную в п. 2.1 последовательность промодулировать методом гаммирования, используя пароль в качестве налагаемой гаммы.

3. Вариант алгоритма генерации ключа длиной 512 байт.

3.1. Записать числа от 0 до 255 в виде матрицы 8*32

0	1	2	.....	31
32	33	32	.....	63
64	65	66	.....	95
.....				
.....				
224	225	226	.....	255

3.2. Установить значение i 0, j 0.

3.3. Установить к=1.

3.4. Выписать столбец матрицы, начинающийся с числа (b_k + i) mod 32.

3.5. Установить j j+1. Если j 64, то перейти к п.3.8.

3.6. Установить к=к+1. Если К≧ 1, то перейти к п.3.4.

3.7. Установить i i+1.

3.8. Накладывая пароль как гамму, промодулировать полученный ряд числе с использованием операции XOR.

Второй этап заключается в выполнении процедур, реализуемых блоками 05 и 06 (фиг.1).

В блоке 05 осуществляется формирование шифрключа из ключа, полученного на первом этапе, в виде подключей заданного размера, которое включает последовательное вычисление значений указателей номера подлежащего обработке блока ключа Y_i и U_i(i 1,2,) по формулам, например:

Y_i [Y_{i-1} + f (U_{i-1})] mod (L_y/K),

U_i [U_{i-1} + f (U_{i-1})] mod (L_u),

где L_y и L_u длины подключей в байтах, определяемых выбранным режимом обработки.

В блоке 06 осуществляется шифрование информационного сигнала по заданному режимом способу, например, путем дискретизации сигнала на блоки длиной 2 и более байт и преобразования этих блоков, например, по следующим вариантам модификации.

В первом варианте (фиг.2) используется, например, метод с двумя непересекающимися подключами, причем в верхнем подключе устанавливается шаг нумерации в 2 байта, а в нижнем 1 байт. В этом случае шифрование осуществляется по формуле

$(C_1.C_k)_i$ [$(t_1.t_k)_i$XORF(Y_i)+f (U_i)] XOR (p+1) (1)

где $(C_1.C_k)_i$, $(t_1.t_k)_i$ - зашифрованные и исходные информационные сигналы i-го блока,

p константа, задаваемая, например при выборе режима.

В другом варианте (фиг.3) для внесения дополнительной неопределенности для криптоанализа с коэффициентом 256 используется, например, четырехбайтовая константа p, вычисляемая по паролю на первом этапе. Механизм преобразований в этом случае заключается в том, что общий ключ представляется в виде 32-разрядных двоичных чисел, а шифрование осуществляется 4-х байтовыми блоками.

В этом случае шифрование осуществляется по формуле, например:

$(C_1C_2C_3C_4)_i$ [$(t_1t_2t_3t_4)_i$ XORF(Y_i) + f (U_i)] XOR (p+1) (2)

Приведенные алгоритмы реализуют режим блочного шифрования, аналогично организуется и поточное шифрование информации, когда каждый символ исходного информационного сигнала преобразуется отдельно. При этом скорость шифрования

RU 2077113 C1

RU 2077113 C1

существенно не меняется. Для сопоставления отметим, что для системы по стандарту DES при реализации поточного шифрования необходимо использование специальных схем, что приводит к снижению скорости шифрования до 25% от скорости преобразования в блочном режиме.

Дешифрование выполняется с использованием выбранного ключа и режима, и этот процесс является инверсией процесса зашифрования.

Дешифрование зашифрованного сигнала включает дискретизацию принимаемого зашифрованного информационного сигнала на к-битовые блоки, Например, при к ≥ 2, преобразование блоков к виду

$(t_i.t_k)$ $[(C_1.C_k)XORF(Y_i) + f(U_i)]XOR$ $(p+i)$ (3)

где $(C_1.C_k)$, $(t_1.t_k)$ константа, задаваемая выбранным режимом.

Формула (3) представляет собой инверсию формулы (1).

Аналогично дешифрование зашифрованного сигнала может производиться преобразованием блоков к виду, например,

$(t_1.t_k)$ $(C_1.C_k)XOR$ $[256f(U_{i-1})$ $+f(U_{i-1}+1)]$ $F(Y_i)$ (4)

где $(C_1.C_k)$, $(t_1.t_k)$ зашифрованные и дешифрованные информационные сигналы. Формула (4) представляет собой инверсию формулы (2). Устройство, реализующее способ криптозащиты систем телекоммутационных технологий, содержит вычислитель 1, блок 2 ввода-вывода, блок 3, алгоритмов, блок 4 хранения ключевых данных блок 5 сопряжения, блок 6 криптомодуля, шифратор 7, блок 8 управления.

Блок 1 вычислителя, который входит в состав рабочего места пользователя и выполняет функции его аутентификации, участвует в программной реализации первого и второго этапа шифрования. Блок вычислителя может быть реализован в виде ЭВМ со всеми периферийными устройствами.

Блок 2 ввода/вывода информации позволяет вводить и выводить различные виды информации, подлежащие шифрованию. С выхода блока 2 сигналы сообщения поступают либо на вход блока 1 либо на 1-ый вход блока 7. На вход блока 2 сигналы поступают либо с выхода блока 1 либо со второго выхода блока 7.

Блок 3 алгоритмов обеспечивает предварительную настройку криптосистемы и предназначен для формирования процедур первого этапа шифрования и установки режимов работы шифрующего устройства в различных вариантах его использования, реализован программно в оперативной памяти ЭВМ. В блоке 3 на этапе настройки в режиме закрытого распределения ключей формируется псевдослучайная последовательность (ПСП) на основе секретного пароля, известного только пользователю (автору) информации, вводимой в систему телекоммуникационной технологии. Сформированная в блоке 3 ПСП записывается в блок 4 хранения ключевых данных. Блок 3 программно обеспечивает выбор режимов работу устройства, позволяющих осуществить простую смену алгоритмов работы устройства в различных вариантах его использования.

Блок 4 хранения ключевых данных реализован программно в оперативной памяти вычислителя и обеспечивает хранение информации о ключах пользователя в виде, гарантированно защищенном от несанкционированного доступа (НДС).

Блок 6 криптомодуля реализован программно и существует резидентно в адресуемой памяти вычислителя. Блок 6 предназначен для выполнения операций шифрования и дешифрования второго этапа криптографических преобразований.

Блоки 3,4 и 6 представляют из себя область адресуемой памяти запоминающего устройства, входящего в состав вычислителя 1.

Блок 5 сопряжения предназначен для реализации протоколов, обеспечивающих сопряжение устройства с каналами связи общего пользования по электрическим параметрам.

Шифратор 7 реализован аппаратно и предназначен для выполнения операций второго этапа криптопреобразований по заявляемому способу.

Блок 8 управления реализован аппаратно и состоит из приемника сигналов Единого времени и узла формирования меток времени.

Формула изобретения:

1. Способ криптозащиты систем телекоммуникационных технологий, заключающийся в предварительной записи в запоминающее устройство совокупности разрешенных паролей, введении пароля, его идентификации, вводе ключа, генерировании псевдослучайной последовательности, формировании шифрключа, шифровании информационного сигнала, передачи в канал системы связи общего пользования шифрованного сигнала и дешифровании этого сигнала, отличающийся тем, что после идентификации пароля вырабатывают сигнал выбора режима обработки шифрключа и информационного сигнала в системе открытого или закрытого распределения ключей, генерируют псевдослучайную последовательность с использованием выбранной системы распределения ключей, формируют шифрключ в виде подключей заданного размера из псевдослучайной последовательности по выбранному режиму, вводят сигналы Единого времени, шифруют информационный сигнал по заданному режиму, передают его в канал системы связи общего пользования и дешифруют.

2. Способ по п. 1, отличающийся тем, что в системе закрытого распределения ключей псевдослучайную последовательность генерируют в виде последовательности чисел и накладывают на нее пароль.

3. Способ по п. 1, отличающийся тем, что для генерации псевдослучайной последовательности в системе открытого распределения ключей вводят ключи первого X_A и второго X_B корреспондентов, формируют две последовательности по формулам

$$Y_A = g^{X_A} \bmod N;$$

$$Y_B = g^{X_B} \bmod N,$$

где g и N параметры открытого ключа, после чего передают сформированные

RU 2077113 C1

RU 2077113 C1

последовательности Y_A в направлении B и Y_B в направлении A, вычисляют общую последовательность вида

$$Y^* = g^{X_A X_B} \bmod N.$$

4. Способ по пп.1 или 2, 3, отличающийся тем, что для формирования шифрключа из псевдослучайной последовательности Y^* в виде подключей заданного размера L_y и L_u последовательно вычисляют значения указателей номера подлежащего обработке блока из псевдослучайной последовательности Y_i и U_i (i 1, 2,) по формулам

Y_i $[Y_{i-1} + f(U_{i-1})] \bmod (L_y / k)$;

U_i $[U_{i-1} + f(U_{i-1})] \bmod (L_u)$,

где L_y и L_u длины подключей в байтах, определяемых выбранным режимом обработки;

$k \geq 2$ число, определяемое длиной подлежащего обработке блока в байтах.

5. Способ по п. 1, отличающийся тем, что для ввода сигналов Единого времени принимают их по каналам системы Единого времени, выбирают из них временные метки по заданному режиму и записывают эти метки в адресные области блоков шифрсигналов.

6. Способ по пп. 1 или 2, 3, отличающийся тем, что для шифрования информационного сигнала по заданному режиму дискретизируют информационный сигнал на k байтовые блоки ($k \geq 2$) и преобразуют эти блоки к виду

$(C_1\ C_k)$ $[(t_1\ t_k)_i$ XORF$(Y_i) + f(U_i)]$ XOR $(p + i)$,

где $(C_1\ C_k)$, $(t_1\ t_k)$ зашифрованные и исходные информационные сигналы,

$p \geq 2$ константа, задаваемая выбранным режимом.

7. Способ по п. 1, отличающийся тем, что для шифрования информационного сигнала по заданному режиму дискретизируют информационный сигнал на k - байтовые блоки ($k \geq 2$) и преобразуют эти блоки к виду

$(C_1\ C_k)_i$ $[(t_1\ t_k)_i + F(Y_i)]$ XOR $[256f(U_{i-1} + 1)]$

где $(C_1\ C_k)$, $(t_1\ t_k)$ зашифрованные и исходные информационные сигналы.

8. Способ по пп. 1 или 2, 3, отличающийся тем, что для дешифрования принятого зашифрованного сигнала дискретизируют его на k байтовые блоки ($k \geq 2$), преобразуют эти блоки к виду

$(t_1\ t_k)_i$ $[(C_1\ C_k)_i$ XORF $(Y_i) + f(U_i)]$ XOR $(p + i)$,

где $(C_1\ C_k)$, $(t_1\ t_k)$ зашифрованные и дешифрованные информационные сигналы,

$p \geq 2$ константа, задаваемая выбранным режимом.

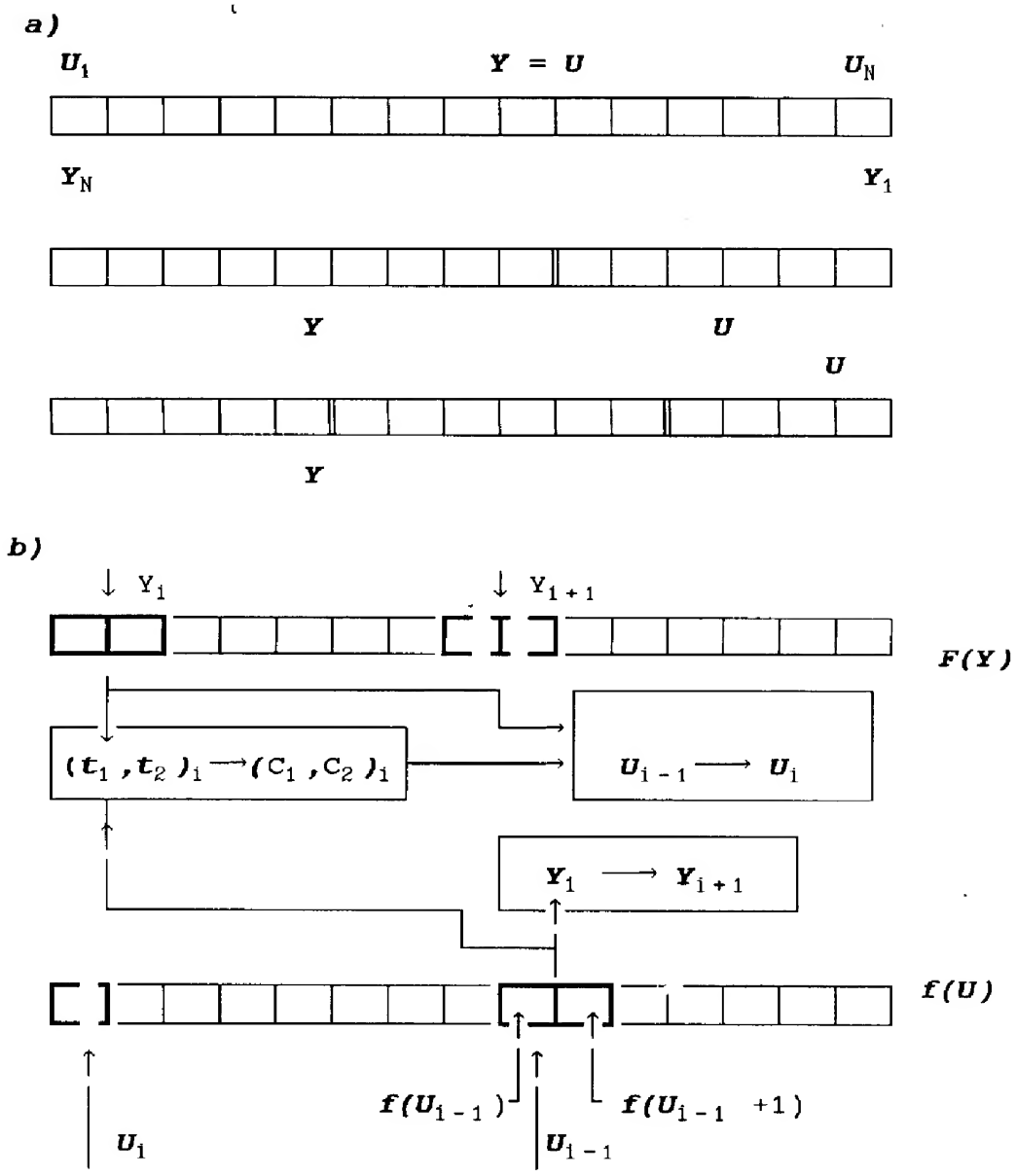
9. Способ по п. 7, отличающийся тем, что для дешифрования принятого зашифрованного сигнала его дискретизируют на k байтовые блоки ($k \geq 2$), преобразуют эти блоки к виду

$(t_1\ t_k)_i$ $(C_1\ C_k)_i$ XOR $[256\ f(U_{i-1}) + f(U_{i-1} + 1)]$ $F(Y_i)$,

где $(C_1\ C_k)$, $(t_1\ t_k)$ зашифрованные информационные сигналы, i 1,2,3

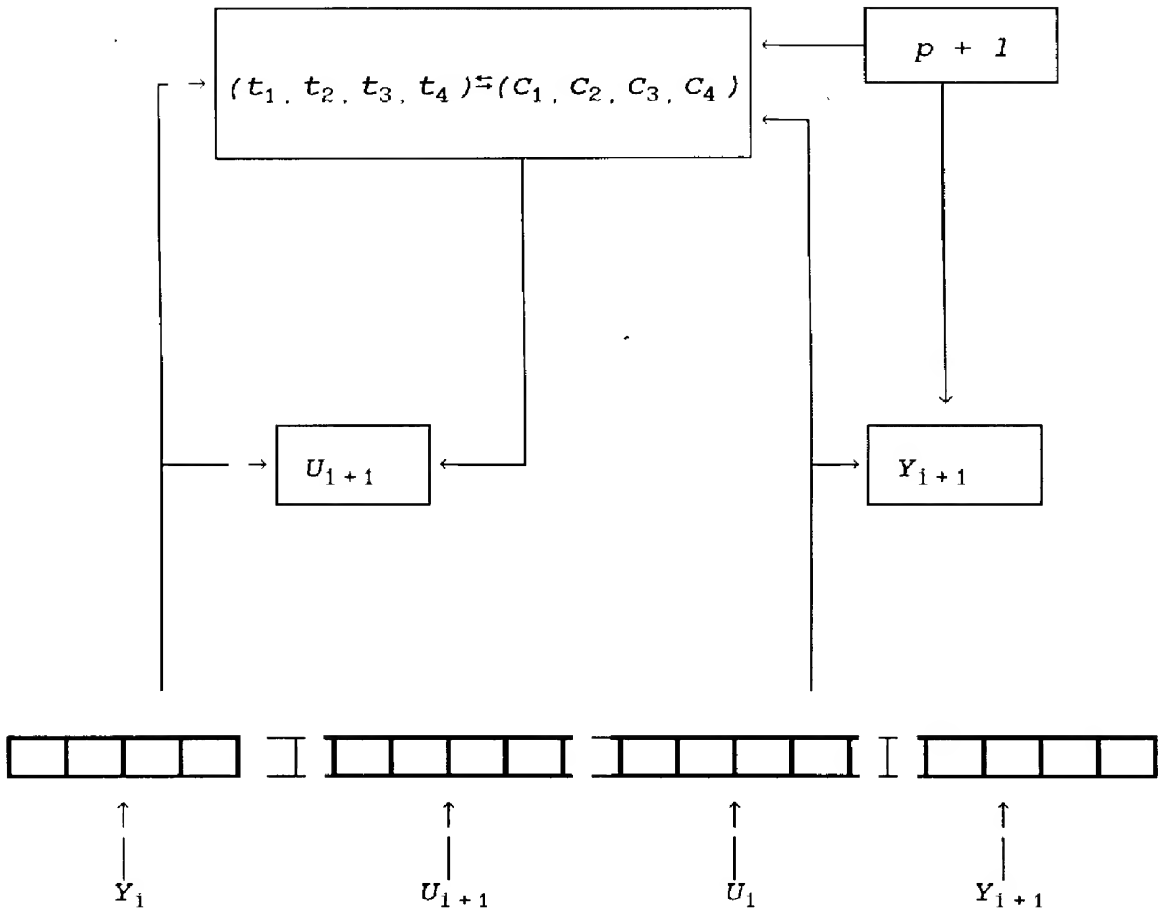
RU 2077113 C1

RU 2077113 C1



Фиг. 2

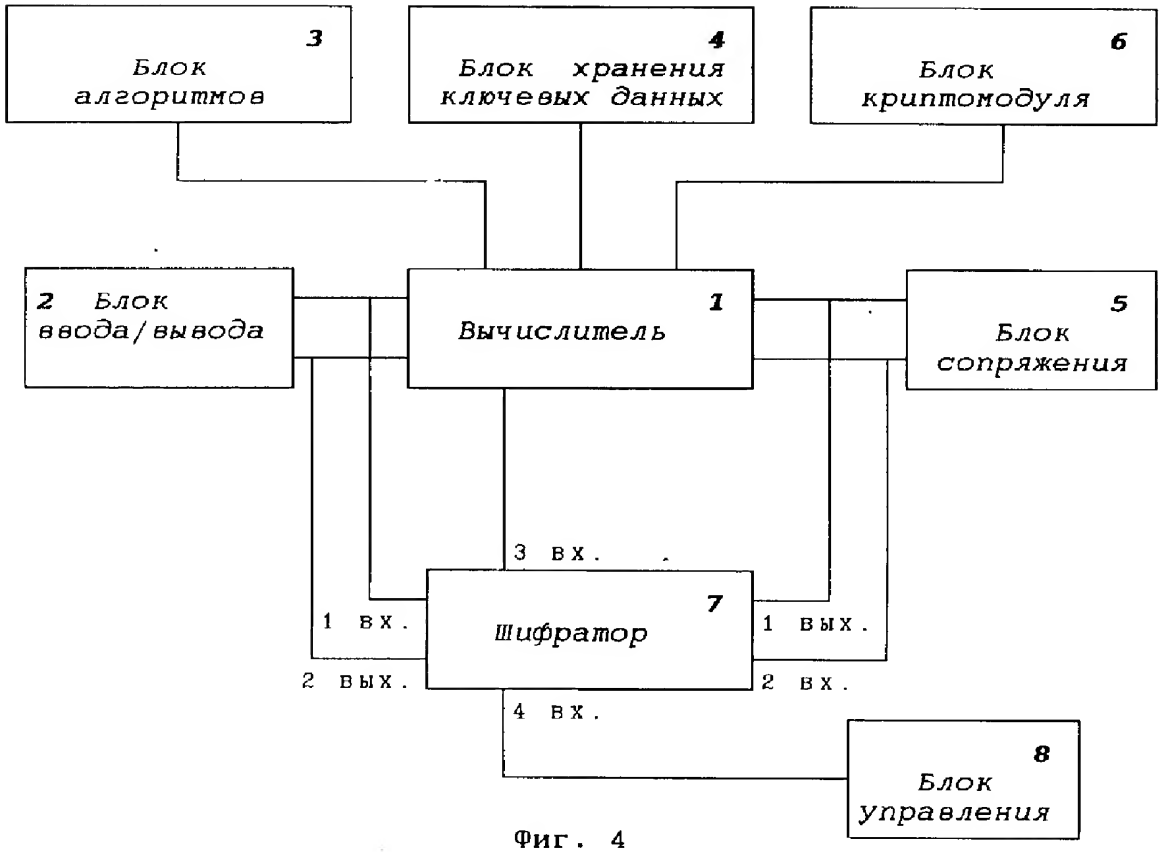
RU 2077113 C1



Фиг. 3

RU 2077113 C1

RU 2077113 C1



Фиг. 4

RU 2077113 C1

RU 2077113 C1